Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Saturday, May 28, 2011

Bitcoin, what took ye so long?

So asks gwern in a spectacular display of hindsight.

The short answer about why it took so long is that the bit gold/Bitcoin ideas were nowhere remotely close to being as obvious gwern suggests. They required a very substantial amount of unconventional thought, not just about the security technologies gwern lists (and I'm afraid the list misses one of the biggest ones, Byzantine-resilient peer-to-peer replication), but about how to choose and put together these protocols and why. Bitcoin is not a list of cryptographic features, it's a very complex system of interacting mathematics and protocols in pursuit of what was a very unpopular goal.

While the security technology is very far from trivial, the "why" was by far the biggest stumbling block -- nearly everybody who heard the general idea thought it was a very bad idea. Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai). Only Finney (RPOW) and Nakamoto were motivated enough to actually implement such a scheme.

The "why" requires coming to an accurate understanding of the nature of two difficult and almost always misunderstood topics, namely trust and the nature of money. The overlap between cryptographic experts and libertarians who might sympathize with such a "gold bug" idea is already rather small, since most cryptographic experts earn their living in academia and share its political biases. Even among this uncommon intersection as stated very few people thought it was a good idea. Even gold bugs didn't care for it because we already have real gold rather than mere bits and we can pay online simply by issuing digital certificates based on real gold stored in real vaults, a la the formerly popular e-gold. On top of the plethora of these misguided reactions and criticisms, there remain many open questions and arguable points about these kinds of technologies and currencies, many of which can only be settled by actually fielding them and seeing how they work in practice, both in economic and security terms.

Here are some more specific reasons why the ideas behind Bitcoin were very far from obvious:

(1) only a few people had read of the bit gold ideas, which although I came up with them in 1998 (at the same time and on the same private mailing list where Dai was coming up with b-money -- it's a long story) were mostly not described in public until 2005, although various pieces of it I described earlier, for example the crucial Byzantine-replicated chain-of-signed-transactions part of it which I generalized into what I call secure property titles.

(2) Hardly anybody actually understands money. Money just doesn't work like that, I was told fervently and often. Gold couldn't work as

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

money until it was already shiny or useful for electronics or something else besides money, they told me. (Do insurance services also have to start out useful for something else, maybe as power plants?) This common argument coming ironically from libertarians who misinterpreted Menger's account of the origin of money as being the only way it could arise (rather than an account of how it could arise) and, in the same way misapplying Mises' regression theorem. Even though I had rebutted these arguments in my study of the origins of money, which I humbly suggest should be should be required reading for anybody debating the economics of Bitcoin.

There's nothing like Nakamoto's incentive-to-market scheme to change minds about these issues. :-) Thanks to RAMs full of coin with "scheduled deflation", there are now no shortage of people willing to argue in its favor.

(3) Nakamoto improved a significant security shortcoming that my design had, namely by requiring a proof-of-work to be a node in the Byzantine-resilient peer-to-peer system to lessen the threat of an untrustworthy party controlling the majority of nodes and thus corrupting a number of important security features. Yet another feature obvious in hindsight, quite non-obvious in foresight.

(4) Instead of my automated market to account for the fact that the difficulty of puzzles can often radically change based on hardware improvements and cryptographic breakthroughs (i.e. discovering algorithms that can solve proofs-of-work faster), and the unpredictability of demand, Nakamoto designed a Byzantine-agreed algorithm adjusting the difficulty of puzzles. I can't decide whether this aspect of Bitcoin is more feature or more bug, but it does make it simpler.

Posted by Nick Szabo at 4:35 PM

51 comments:

Zooko said...

What private mailing list was that?

10:10 PM

nick said...

libtech

10:23 PM

Daniel A. Nagy said...

In my opinion, BitCoin has not one, but several outstanding ideas in the ways of combining well-known cryptography. Yet, I believe that it is a bubble that is going to burst due some crucial deficiencies.

Strokes of genius include:
- The formal language used to describe transaction details. Smart contracts right there!
- The trick of including useful information (the transaction list) in the data to be hashed for finding hashes from a small set.
- The voluntary transaction fee.
- The way they deal with Moore's law by adjusting difficulty.

However, I am still skeptical and expect the outcome to be the cheap graphics cards to be dumped on the secondary market soon.

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ▼ 2011 (12)
  - ► December (1)
  - ► July (1)
  - ► June (2)
  - ▼ May (2)
    - Bitcoin, what took ye so long?
    - Lactase persistence and quasi-pastoralism
  - ► February (2)
  - ► January (4)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ► 2006 (130)
- ► 2005 (44)

This is due to several -- in my opinion fatal -- flaws in BitCoin:

* Almost all mining currently occurs in two large mines, where shares are not self-enforcing smart contracts written in BitCoins transaction language (it is not suitable for that yet), but relies on the mines' operators as trusted third parties (by popular definition: ones that can violate the security without getting caught). Thus, in practice, BitCoin network is not as decentralized as many think it is.
* The transaction protocol does not scale beyond small transaction volumes, making it unsuitable for direct use as payment by many users. Another problem is the 10 minute confirmation time for transactions. This makes it also vulnerable to DoS attacks.
* By making computational capacity directly monetizable, it creates all sorts of agency problems for organizations with lots of it. Currently, it is not clear how to prevent employees with access to big data centers from stealing their employer's computational power for mining BitCoin for themselves. Appropriate defensive measures may well be prohibitively expensive.
* With no guaranteed baseline demand (redundant backups of a few hundred kilobytes is not enough), it is possible for BitCoin to become completely worthless.
* It's hugely wasteful in terms of computation.

But I still believe that BitCoin introduced many useful ideas that will be applied in successful crypto-currencies.

7:22 AM

nick said...

Daniel, your points about the security may be valid, (I haven't audited the code, and it could certainly use such an audit). And on top of this I'd add the copious legal risks. But I'm afraid the economic points are another matter.

As for the long transaction delay and poor scalability, I long considered bit gold as a design for "high-powered money" that like gold could be used as an investment vehicle, a medium for large transactions, and a reserve currency against which digital notes could be issued. It would be however be far more securely auditable than remote gold vaults. If you're right on this critique Bitcoin may be destined to become a high-powered money rather than a day-to-day payment system for the masses.

The computational cost issue is as I've shown in my above-linked account of the origins of money a red herring. As with gold, the mining cost gets amortized by the function of bit gold in lowering transaction costs, both as a store of value and a medium of exchange. If somebody figures out how eliminate creation costs of a digital currency without reintroducing an incentive to inflate I wish all power to them, but I'm not holding my breath.

And what's up with the term "cryptocurrency"? What is it supposed to mean? Cryptography is used to protect payments systems as radically different as credit cards, Chaumian digital cash, and Bitcoin. The term encourages the popular but profoundly naive view of Bitcoin as merely another form of digital cash.

As for whether it's a bubble, any collectible market can turn into a bubble. It's the nature of the beast. But at the current prices and supply, the amount of Bitcoin (last I heard about $40 million in USD terms) was still very small compared to many other collectible markets, much less the amount of currency in circulation from the central banks of even tiny governments. Bitcoin certainly has major downside risks but it also has far more upside potential than other collectibles. So obviously it's an extremely risky investment at this point in time. Nobody should be doing anything remotely close to what I read this morning from some twitterer (presumably it was just prevaricating puffery) and putting "all [his] money" into it. It's a curiosity collectible, an alternative to a small fraction of one's gold holdings as a hedge for fiat-denominated debt, and a medium of exchange for at least certain niche transactions. And potentially much more.

12:49 PM

Daniel A. Nagy said...

Okay, let's call BitCoin a digital commodity, which is certainly a more accurate term. I certainly agree with you that it has better

chances at becoming an investment vehicle than a day-to-day currency.

I have read and even popularized your "Shelling out" essay (moreover, this fall I am looking forward to discussing it with students in Kyrgyzstan, just to refer back to our previous conversation) and I fully agree with what you write there. However, there is a crucial difference between gold and BitCoin: the negative feedback that keeps gold price stable at (actually -- for some reason that I do not quite understand -- below) marginal expected mining effort is that if gold becomes too expensive, more effort will be put into mining thereby increasing supply, while if gold price falls, people stop mining. With BitCoin, there is no such feedback: no matter how much effort is put into BitCoin mining, the rate at which BitCoins emerge is near constant. When BitCoin becomes (as it is right now) very expensive, people start devoting more processor power to mining, but they actually do it at other miner's expense: they will mine more and everybody else will mine less. The supply of BitCoin will not increase due to increased activity. BitCoin can eat all the processing power in the world due to this competitive/adversarial setup.

Thus, unlike gold, where the cost of mining effort is relatively stable and the market price fluctuates around it, in case of BitCoin, mining effort follows market price without any feedback. Now that BitCoin is very expensive (compared to the cost of mining), processing power devoted to mining is growing like crazy, doubling roughly every month. Eventually, the cost of mining BitCoin may catch up with its market price. But it will have no stabilizing effect on it.

Similarly, if BitCoin price starts falling, miners will free up computational capacity (that's when I expect cheap second-hand graphics cards to hit eBay en-masse), but that won't decrease supply. And unlike gold, which is pretty and instinctively desired, there is no bottom to this market. BitCoin can easily become totally worthless, as no matter how little computational capacity is devoted to mining, bitcoins will keep coming at a 5 BTC / minute rate.

1:21 PM

nick said...

I certainly agree with you that it has better chances at becoming an investment vehicle than a day-to-day currency.

Hmmm, I'm not sure that's quite what I meant to say. If your critique of scalability and transaction times is correct, I do agree that it won't be a payment system for the masses. However, as a high-powered money it can still be a currency, with a redemption window where digital bank notes (the payment system for the masses) can be redeemed for Bitcoin. But it's all the same currency, just as both a pound of silver and bank notes redeemable for a pound of silver (or its gold equivalent) were once the currency of the British Empire. Securely auditable Bitcoin held by the note-issuing banks would greatly increase their trustworthiness.

if gold becomes too expensive, more effort will be put into mining thereby increasing supply, while if gold price falls, people stop mining. With BitCoin, there is no such feedback: no matter how much effort is put into BitCoin mining, the rate at which BitCoins emerge is near constant.

I think this is a valid critique. For the reasons you state Bitcoin is far more susceptible to radical deflation than gold. Sufficiently high deflation can bring credit markets to a halt as real interest rates become higher than the time and risk value of money a market in a non-deflationary market would set. If people figure out how to make loans at negative nominal interest rates, that would help solve this problem, but that only handles expected deflation; it wouldn't prevent widespread bankruptcies and other problems that come from unexpected radical deflation.

My bit gold design would work very differently than Bitcoin in this regard -- the relative prices of solution bits between periods of time (e.g. between one week and the next) would be set by a market, not by a prescheduled algorithm, so as with gold supply would be able to adjust to meet greater demand.

2:15 PM

Daniel A. Nagy said...

It's not just deflation against which BitCoin is defenseless. Given the lack of feedback, it is just as susceptible to inflation: Suppose that mining costs catch up with market price. Then, for some reason, market price falls as people sell off their BitCoins. Some miners stop. Some may even sell their equipment and quit the network altogether. This will not reduce the supply of BitCoin, just makes the system a bit more fragile. Those who stay in the mining business will see their rate of mining increase, and rationally anticipating further fall in prices, will also increase the rate at which they sell BitCoin, fulfilling their expectation.

People with BitCoin savings liquidate, some businesses stop accepting BitCoin.

BitCoin's market price falls further. The limit is zero. No feedback to stop the ensuing inflation caused by the general shrinking of BitCoin economy. More and more BitCoin chasing fewer goods and services (and currencies).

This is what I actually expect to happen after the current bubble bursts.

3:00 PM

Daniel A. Nagy said...

Your proposed design with different vintage bit-gold having different floating prices will make it essentially useless as an accounting unit, which is an important function of any currency.

But thinking about digital commodity design is by no means futile. I believe that BitCoin is just a first attempt which will be superseded with better designs. It is also sufficiently flexible to be able to change the rules, if necessary. For example, not allowing difficulty to ever decrease would be a good move. The risk is that clients that do not upgrade will fork the block chain, since they will find "easy" hashes faster in case of a scheduled decrease by the old (current) rules.

3:12 PM

nazgulnarsil said...

One issue I haven't been able to wrap my head around so far is the fact that bitcoin holders themselves don't have any decision making power in the network. The people with the power to confirm/deny things are the masses of people running clients and the people with the most hashing power. while these are *generally* the people with a lot of bitcoins this doesn't necessarily have to be the case. It seems tha, like with a joint-stock company, you should need to have a vested interested to be able to make decisions. The people with the most bitcoins have the highest incentive to prevent fraud, therefore they should have the power. gmaxwell pointed out on #bitcoin that bitcoins can easily be traded for either hashing power or the ability to spam lots of client nodes (bot nets). But this still strikes me as odd. You don't have to sell your stocks to exercise the voting power.

5:10 PM

nick said...

Daniel, that's a good explanation and I agree it makes Bitcoin inflation risks worse too.

I do have solution to the unit of account problem:

"Bit gold will be entirely public: no one gains secure title to any puzzle solutions until they are published. Thus, the exact amount and kind of puzzle solutions during a given period are well known, and perfectly define the supply curve relative to future weeks for all time thereafter...To create fungible units dealers will bundle strings of different value into pools of a standard value (i.e. collect strings into a pool so that the sum of the market values of the strings in the pool add up to the standard value)...there are no ongoing changes in subjective valuations [or differences in security properties] between bit strings [of different periods] to worry about, but instead the demand for bit gold is purely for its monetary functions, and thus purely based on how scarce the supply of puzzles solved during a given time period was and is...[thus] The supply and demand curves of different pools will change in the same way over time, and the relative values of pools will not diverge from their initial relative values. Using tranches as standard denominations for

a currency [thus] does not create arbitrage opportunities."

5:14 PM

nick said...

nazgulnarsil, it doesn't readily come to my mind what conflicts of interest miners might have with other stakeholders (which I tend to think of as holders, creditors, and debtors). What biases on their part did you have in mind? Current Bitcoin or bit gold holders do have a bias towards deflation. Albeit this historically has not been as big a problem as inflation, they and creditors do have a conflict of interest with debtors.

Your objection does suggest to me an interesting possible improvement in the Byzantine agreement security. Instead of, or in addition to, the Byzantine "voting power in case of civil war" going to those proving work (i.e. the miners), require that participants sign challenges with their ownership keys to prove they own solution bits. The behavior of conflicting sending nodes, when the receiving node can't otherwise distinguish between correct and incorrect behavior, then gets weighted by the value of solution bits owned by said sender, either par or market, or similar. With such method one would have to own most of the money in circulation, rather than just most of the mining power, to corrupt the system (i.e. to successfully attack the subset of features that only have a Byzantine rather than cryptographic level of protection). This would discourage anonymity since doing these signatures and verifications over many keys would get computationally intensive, but I don't think strong anonymity is a feasible property in bit gold or Bitcoin anyway.

5:52 PM

Daniel A. Nagy said...

Nick, but then how your solution is substantially different from what BitCoin is doing? If the standardized value is inversely proportional to the number of puzzles solved during a week, we're back to the problem of lack of feedback: when some people stop mining, those that continue will see the value of their finds go up (in standard units), instead of the standard unit itself becoming more valuable.

11:22 PM

nick said...

If the standardized value is inversely proportional to the number of puzzles solved during a week,

I don't think this will happen. The market will set the relative value of a solution bit from one week to a solution bit from another week based on what people believe the relative cost of solving a bit was between those weeks. If the value of the standard bundle falls causing some miners to drop out, the profit margin of the remaining miners remains as it was after the value fell but before the miners dropped out.

Weeks when the standard bundle goes down there may be very little production (with that week counting for very little in the standard bundle) whereas weeks where the standard bundle goes up there will be abnormally large production and a correspondingly high number of solution bits from that week incorporated into the standard bundle. A very interesting issue though!

12:44 AM

Daniel A. Nagy said...

This comment has been removed by the author.

5:01 AM

Daniel A. Nagy said...

Nick: then I must admit to not understanding what you propose. If we're having a fungible commodity, it means that the title registry essentially assigns a non-negative balance to each public key with the private pair of which transfers need to be signed. When someone presents a proof of work, their balance needs to be increased by some value without decreasing any other balance. How that value is to be determined from the information available?

The only available information is a reasonable estimate of the amount of hashes attempted for this find and each find in the past.

BitCoin has a function that does not depend on any other input. You propose some market mechanism that will come up with a number after a limited amount of time?

5:13 AM

nick said...

Daniel, I suggest reading the bit gold description more carefully. There are no balances in the underlying bit gold system. Just replicated chains of titles to solution bits. Because these solution bits are not fungible between one period and another, on top of this I propose bit gold markets, consisting of

(1) markets that set relative prices between the solution bits of one period and another, and

(2) dealers who use these market prices to bundle solution bits from different periods into bundles of standard value, creating a fungible commodity, which is then used as the currency.

Taking commodities of different qualities and quantities and making bundles of standard value is an art common to most commodity markets, and here the task is easy because markets set the prices for the different periods. Admittedly, I've specified the bit gold market layer in much less technical detail than the underlying bit gold layer because there are many design choices that could be made and I've been focusing on the economics rather than the computational and security mechanisms of the higher layer. Still I think the basic scheme is clear enough.

12:21 PM

nick said...

Here is an example of how to implement a payment system based on bit gold and bit gold markets: if one wants the payment system for the masses to be in the form of scalable digital bank notes, issued by competing banks with securely auditable reserves, note-issuing banks can also play the role of the dealers as follows:

(1) the bit gold market sets the different prices for the different periods, as before

(2) banks own solution bits which being in the public replicated title registry are securely auditable

(3) competing banks issue digital bank notes redeemable in solution bits whose market values add up to the face value of the bank note (i.e. they create bundles of standard value)

So the auditing software in step (2) checks the market prices to compute the desired total values of solution bits. The bank software in step (3) goes through the title database to discover solution bits that add up to the face value of the note, and the bank client's software also checks the market prices of these bits to keep the bank honest.

The note-issuing banks are a minimal intrusion of trusted third parties (TTPs) because they are securely auditable and the underlying assets are bit gold which depend on distributed Byzantine agreement and cryptography rather than singular TTPs.

Notice BTW that we still don't need expressly represented accounts or balances. Any such is an optional add-on feature. The total value of what a key owns is implicit in the public title database but must be computed using the market prices of the owned solution bits.

Those familiar with the free banking of yore will observe that the above is a pretty good analog of the banks that issued bank notes redeemable in gold reserves.

12:56 PM

Daniel A. Nagy said...

Nick, I have re-read your bitgold essay and I still feel that I am missing some important detail where "*the bit gold market sets the different prices for the different periods*". How? The only information that it has is the amount of bitgold mined each week.

Suppose, I mine a "this week bit gold nugget". Do I put it up for auction where bidding is done in "last week bit gold nuggets"? Does trading occur before, during or after "this week"?

There rest is easy and I do understand that part.

1:51 PM

nick said...

How? The only information that it has is the amount of bitgold mined each week.

There's a heck of a lot more information than that. For example, traders know the prices of bit gold vs. precious metals and other currencies, thus can make good estimates of the current value of bit gold. Based on bit gold production and public technical information they can make pretty good guesses about what it costs or cost during a period to mine bit gold. Knowing this information they can make good estimates of miners' profit margins. Those are a few but far short of all the kinds of information traders will have available to bargain with miners and each other to set the different prices of the different periods.

I'm puzzled, BTW, that your contribution to this discussion seems to consist solely of criticisms rather than positive suggestions for improvement. Many of the criticisms are interesting and I appreciate them, but you would come across quite a bit better if you tried to propose solutions to at least some of the problems you raise, instead of seeming to suggest that they are insoluble. Since I have in fact solved many of them, and nobody has made a good argument showing that the others can't be solved, such a conclusion would be quite silly.

3:03 PM

Daniel A. Nagy said...

Oh, I am not suggesting that these problems are insolvable. Moreover, I think that precisely because they probably *can* be solved, BitCoin is not the last word in digital commodities. It will either improve or get superseded by a better solution.

But they are hard. BitCoin solved many problems in absolutely ingenious ways and as a result it is a moderate success. In order to improve on it, we first need a good assessment of what is good and what is bad about BitCoin and even that is far from obvious.

Furthermore, while I agree with the general sentiment that we are on the verge of a new era in payment, I am not convinced that digital commodities are the right way forward. Primarily, because commodity money has actually historically lost against pure credit money, so its superiority is not indisputable. Thus, I am also interested in de-monopolized pure credit money. A mixed monetary system may also be interesting.

1:15 AM

The pwnage ahead said...

@Daniel:

** Almost all mining currently occurs in two large mines, where shares are not self-enforcing smart contracts written in BitCoins transaction language (it is not suitable for that yet), but relies on the mines' operators as trusted third parties (by popular definition: ones that can violate the security without getting caught). Thus, in practice, BitCoin network is not as decentralized as many think it is.*

Not true at all. As has been discussed numerous times by the developers and in the original paper that created the basis for Bitcoin, a fork in the block chain would not go un-noticed. Rather, it would be seen by everyone in the network and would exist for the amount of time that an attacker could control the entire network. It could be done, but for how long - 20 minutes? Eventually the power of the network would overcome this problem and let the light of truth shine in on what happened - unless of course someone came in with 80 or 90% of the existing network's hashing power - not likely considering that Bitcoin now surpasses the power of the world's top 500 supercomputers combined (see the Bitcoin forums for citation). Although it remains to be seen what other yet-to-be-discovered technical weaknesses are present, other than that which you described.

** The transaction protocol does not scale beyond small transaction volumes, making it unsuitable for direct use as payment by many users. Another problem is the 10 minute confirmation time for transactions. This makes it also vulnerable to DoS attacks.*

This is completely false and has already been discussed ad-nauseum on the forums; Bitcoin has enormous scalability. But I have a feeling it's transaction volume will never grow to that of Mastercard's, for example, although the network can easily surpass Mastercard's transaction volume.

2:59 AM

Daniel A. Nagy said...

@Pwnage:

Please read what I have written carefully before responding. The fact that pooled mining is a leap of faith is an undisputed fact, advertized by the pool operators thesmelves. From the horse's mouth:

"*In theory, as the Bitcoin pool operator, I could keep the 50 BTC from a block found by the pool for myself. I'm not going to do this, but I completely accept that people do not trust the pool operator. It is their freedom of choice, and Bitcoin is about freedom.*"

Since most mining occurs in two large pools, these two pool operators have an enormous amount of trust invested in them. Even if the miners continually and automatically audited the pool's operations and left the pool immediately, as soon as they discovered cheating (which at the moment, they don't), a coordinated attack on the two large mining pools would deal a huge blow to the BitCoin system.

This is not a fatal flaw, however and it can be fixed in numerous ways. First of all, if the pool is able to operate with lower difficulty, so could the main block chain. Pooled mining solves a problem that is simply a mis-parametrization of the BitCoin protocol. But even if we accept that BitCoin is the way it is, a smart enforcement of the pool contract and immediate, automated switching to alternative pools in case of breach would solve the problem. One could also solve this problem by extending the transaction language of BitCoin in a backwards-compatible fashion so that it would enable proactive rather than reactive enforcement of the pool contract. In short, the problem can be solved, but currently it isn't.

As for scalability, no, it doesn't have enormous scalability. It may have it in the future, if a few problems get sorted out. Again, you need to go no further than the official BitCoin wiki for a honest discussion.

At the moment, there is an artificial 7tps limit in place in order to prevent abuse. It is not even entirely clean how to coordinate the

removal of this limitation.

Currently, even in peak periods the transaction volume is something like 0.3 transactions per second, sustained for a few minutes.

7:29 AM

nazgulnarsil said...

I haven't studied the source code intensively so I'm not sure about the technical merits of such attacks. It just struck me as odd that a simple majority rather than a qualified majority was implemented to begin with when Satoshi seemed have thought everything else through quite well.

12:09 PM

nazgulnarsil said...

also I don't think it has to be a proportional vote using private keys all the time. It could be a manual thing that only comes up under circumstances that merit it i.e. being attacked.

basically give the holders of large wallets significant veto power in case of emergency.

12:46 PM

Calle said...

Another possible, additional explanation for the "why now?" question is that more people around the planet are seeking alternatives to official currencies that no longer seem as safe in light of the crisis of 2008 and the ongoing economic problems in Europe. (This, in fact, may be driving up demand for gold too.) The zeitgeist, in other words, is right.

I've posted some thoughts on the matter here: http://cs702.wordpress.com/

3:04 PM

nick said...

nazgulnarsil, that's basically the only time the "voting" matters, in an emergency when there are errors in the network corrupting the messages (unlikely) or (more importantly) an attack where nodes intentionally corrupt important properties of the protocol that aren't cryptographically protected.

There are also out-of-band reactions that can occur even if a majority corrupts the system. For example a minority can fork the block chain in Bitcoin (or title registry in bit gold) and then try to convince the world that their transaction history is the correct one and that the corrupt majority is in error. However, it's not clear what kinds of things can be proven out-of-band; this is a topic that deserves much further study.

Canonically Byzantine agreement assumed each node had a secure true-name identity, but because privacy is a desiderata, and because it would be very difficult to implement such a secure identity system on the Internet, we have to use some characteristic of users provable within the Bitcoin or bit gold system to weigh Byzantine "votes". I've now come up with a list of provable attributes in Bitcoin (or bit gold) by which message correctness "votes" might be weighed:

* proof-of-work/mining effort (what Bitcoin currently does)
* value or number of coins or solution bits owned by key
* number or value of transactions as payor, payee, or both by a key
* number or value of transactions weighted by how recent they are

* various combinations of the above

This is an incomplete list, especially if we add new attributes. One of the general ideas here is to weigh Byzantine "voting" towards those with more experience in the system, making a novel invasion more difficult. However in a currency there should also be a balance between various stakeholders (holders, creditors, and debtors). Since Bitcoin- or bit gold- denominated contracts generally exist outside the system, one would have to, at the very least, publicly register those contracts signed by the parties' keys for creditor or debtor status to be provable.

3:18 PM

nick said...

Calle, I agree that the greater unreliability of fiat currencies in recent years may also be a factor. I wrote about the price of gold and commodities in this context here.

3:28 PM

nick said...

I should add, critiquing my own idea, that most of the attributes I list just above are not fully provable with cryptography but in part rely on Byzantine correctness.

For example, a majority attacker can prune the transaction chain to reduce the value of his opponents' coins (or solution bits in bit gold) and thus his votes. Fortunately the majority can't *add* value, at least in bit gold: it does require proof of work to _add_ solution bits and owner signatures which no majority can forge to receive solution bits from others.

It would be worth studying this in more detail -- does the attacker already need to have reached a majority in order to launch a vote-altering attack, rendering it irrelevant, or does the asynchronous nature of the protocol provide a way for a minority attacker to exploit the lack of cryptographic proof to bootstrap their way to a majority? I suspect a much more detailed look at the protocol is required to answer this question.

gwern, are you reading? Most of this stuff is indeed far from straightforward. :-)

Also, one of those annoying edge cases is how the system can safely bootstrap starting with zero coins and zero transactions.

4:11 PM

Calle said...

Nick -- thank you for your response; I've added your post on commodities to the top of my pending-reading list. Great blog, BTW.

7:11 PM

nick said...

Thanks Calle.

2:01 PM

eddie said...

Nick, about your idea for combining diversely-timestamped bitgold into fungible tranches: I believe I understand it in general, but I have a couple of questions I hope you could answer for me.

For clarity (I hope), I'm going to call a solved bitgold puzzle a "grain" and a fungible monetary unit consisting of a bundled tranche of solved bitgold puzzles a "coin". I'll call people who generate solved puzzles "miners" and people who bundle puzzles into tranches "mints".

As I understand your scheme:

Miners will generate grains, but different grains - even grains of the same size - may have different mining costs. Some miners may have better algorithms or more cost-effective hardware. And the cost of mining is certain to drop over time. But given the size of a grain and the time at which it was mined, one can estimate its probable cost. Grains of a given size from different miners mined at approximately the same time (within the same window of a week, or day, or minute) are fungible; grains across different time periods are not.

Mints will generate and/or purchase grains of various sizes and vintages, then combine them into coins. They will then sell the coins or use them in commerce. As with any currency, the value of a coin may fluctuate over time, but all coins will have the same value at any given point in time.

Furthermore:

I believe you have implied that mints will create coins using grains with equivalent total *cost*. If 1024-bit grains from Jan 1 2010 are estimated to have cost their producers 5 cents each, and those from Jul 1 2010 are estimated at 2 cents, then mints would make coins out of 20 of the former or 50 of the latter (for example).

If I've got all that right, then here are my questions:

How do the mints determine how many of which grains to mint into a coin, and how do users determine that a coin has the right set of grains?

Using my previous example: if a mint estimates that January grains cost 5 cents each to produce and July grains cost 2 cents each to produce, then they know how many of each they need to mint a $1 coin. The size of coins ($1) can simply be an agreed-upon standard by the participants. But how can multiple participants - mints and users - jointly determine how much the grains in any given time period cost?

You suggest that the prices of grains will be determined in a market, but I don't understand how such a market would come about. If a mint needs N grains from April to make a $1 coin, then they'll pay $1/N for each one. But the number they need depends on the price they pay! There's too many variables and too few relationships here - something's left unspecified.

Are you suggesting that someone other than mints will be buying grains? If so, that would create a market price which the mints could use to determine how many grains to put in a coin. But I don't see who else would be buying them, as grains themselves seem to have no use outside of being put into coins.

Thanks in advance for any insight you can provide.

5:40 PM

nazgulnarsil said...

I posted my comments and your responses on the bitcoin dev forum but I'm not sure anyone besides me thinks this is a serious issue.

to me this is like a large company ignoring all of its stockholders in a vote in favor of the votes of employees and customer surveys.

3:49 AM

nick said...

nazgulnarsil, that led to some good comments. As Stefan Thomas points out it's easy to do dummy transactions, so that's probably a poor choice, although they discuss how transaction fees might work.

As long as I'm brainstorming suggestions for Bitcoin here are some more:

* The security of the timestamps would be improved if many of the time-stampers each ran their own independent atomic clocks, which recently were selling as add-on cards for about $1,500, rather than relying on third party time services, which is what you're doing if you just use the system clock.

* Same as above, but establish an independent, Byzantine-agreed P2P, atomic clock time-stamping service which could be based mostly on code from Bitcoin. "Bittime", natch. :-) This would provide a more secure Internet time service for everybody.

* To improve transaction rates, reduce time windows for attackers, and provide a backup to the normal Internet connections, high-power nodes (the ones doing lots of mining) might consider doing shortwave radio broadcasts. They might broadcast either summary information by which to know a transaction is coming and then to check the integrity of that transaction, or (with sufficient bandwidth) broadcast the entire chain. One might also weight the Byzantine "votes" higher for messages received by such a direct physical connection.

* If "mining oligarchs" become a reality, they should run code that other participants can audit, using secure hardware that implements remote attestation. Hal Finney's RPOW relied completely on remote attestation but most secure is a combination of remote attestation and the Byzantine agreement of Bitcoin (and of course crypto for those attributes where that stronger form of security is possible).

2:44 PM

nick said...

Yet another idea: use the Bitcoin code to implement secure property titles.

Secure title registries will be used to register ownership of names, name/address bindings, bit gold (solution bits to proof-of-work challenges), and anything else that can be represented as bits and whose ownership needs to be securely agreed to across trust boundaries according to a securely agreed and followed set of rules for claiming (homesteading), transfer, etc.

There is a similar but more specialized project, namely Dot-Bit and namecoin, to implement a secure DNS.

3:12 PM

nick said...

eddie, good questions. I'm obviously still figuring out the best way to explain this, so hopefully this one will do the trick.

(n.b. I've been using "bank note" instead of "coin" and "bit gold" or "solution bits" instead of "grains", and "issuer" instead of "mint", and there are good reasons I chose this terminology, but for the purpose of this response I'll use your terminology).

How do the mints determine how many of which grains to mint into a coin, and how do users determine that a coin has the right set of grains?...You suggest that the prices of grains will be determined in a market, but I don't understand how such a market would come about.

It's more than a suggestion. The "mints" (issuers) don't decide this for themselves, the traders on the inter-period exchanges do. The value of one unit of the currency is defined as the value of a canonical number of bits in the "grains" of some canonical period. So for example, the value of 1024 bits of grains in week 1 (the "genesis grains"). However grains from other periods are used to actually

redeem "coins".

The market comes about as with other collectible markets. For example traders in rare postage stamps estimate how much luck was involved in the variety of printing errors that occur in the stamps most prized by collectors. The difference from collectible stamps being that the markets in "grains" (solution bits) will be far more liquid because trading will be largely automated with instant online clearing, because it's being used as reserves for a currency, and because it's simplified to trading between periods (probably weeks) rather than trading between individual stamps or "grains".

But the number they need depends on the price they pay!

The specific grains in the bundle are determined when "coins" are redeemed, not when they are issued ("minted"). The mint/issuer can be audited at issue time (or any other time) to see if they have sufficient reserves of grains to cover the "coins" they have issued, but they don't distribute these reserves unless the "coin"/"bank note" is redeemed.

Each "coin" is most akin to a digital promissory note (this is why I call them "bank notes"): I promise to redeem "coins"/"bank notes", on demand, for grains adding up to the standard value at the time of redemption. Since the prices of grains are all public, the redeemer and issuer/mint can each look up the market prices of the grains at that time and verify that they add up to the standard value. Determining the relative prices is obvious. The abolute value of a grain created in a given week is determined by comparing the price of grains created in what week to the price of a canonical time period (e.g. the week 1 or "genesis grains".) So the value of one "coin" of standard value can be defined as "the value of 1024 bits of genesis grains", but when you redeem the "coin"/"bank note" it gets redeemed in later grains according to their relative market prices to the genesis grains, which both sides of the redemption transaction can verify.

4:51 PM

nick said...

Another thing to think about wrt the inter-period markets: besides the speculators who will do much of the estimating of how much production cost in each period, the main players in these markets will be the miners and the issuers (mints). Miners will exchange newly mined bits (grains) for earlier ones. The earlier grains, which have a more mature market values, can than be held or spent by the miners or exchanged for other currencies. Mints (issuers) will buy more grains (solution bits) for reserves as they issue more coins (bank notes). The miners thus create the supply of grains and the mints create much of the demand. There will also be demand for bit gold (grains) simply as stores of value in themselves, just there is demand for precious metals and collectibles as such, but even if we ignore such investors, we have parties creating supply and demand and thus a market for each period.

5:23 PM

eddie said...

Thanks for the explanation; that clears some things up for me. The key piece of information was that bank notes would be issued with a face value of a certain number of bits of a canonical reference vintage. Also, clarifying that the bundles are promissory notes to be redeemed later rather than actual bundles of specific mined bits was very helpful.

I appreciate that documenting your bitgold ideas is a work in progress; given the recent interest in BitCoin, you may now have a good opportunity to engage others interested in bitgold and related ideas.

8:01 PM

eddie said...

In your view, does money need to be unforgeably costly, or is it enough for it to be unforgeably scarce? I ask because I can envision digital commodities which are the latter but not the former. Also, I think the answer has implications for a commodity's cost to produce versus its market value - implications with different consequences for BitCoin and bitgold.

8:14 PM

eddie said...

I think your explanation of the inter-period market would benefit from an example. Suppose the following:

* The bitgold software is released. In Week 1, X miners produce a total of Y bitgold solution bits.

* In Week 2, a new algorithm is discovered which produces solution bits twice as efficiently; also, due to publicity on the Internet, ten times as many miners have started mining. So in Week 2, 10X miners produce a total of 20Y bits.

* In Week 3, Amazon announces a price cut on their EC2 rent-a-computer service, which cuts the cost of mining in half again. And continued publicity sees yet another tenfold increase in miners. So in Week 3, 100X miners produce 400Y bits.

* Suppose the standard note is defined as 100 bits of bitgold mined in Week 1, the canonical genesis week. Suppose the market price of standard notes has been holding steady at $1 per note.

Given this simplified example: if someone were to redeem a note during Week 3, how much would you expect the issuer would have to pay for each of the different vintages of bits, and how many of each vintage would they have to purchase in order to make good on the note?

The Week 1 bits seem straight-forward. I could trade a dollar for a note on the external market, and trade a note for 100 Week 1 bits at some issuer that already had those bits on hand, so I'd be willing to trade those bits for a penny each to an issuer who needed to buy them to redeem their own note. (This all ignores profit, of course.)

The Week 3 bits seem straight-forward as well. It costs the miners a quarter-cent per bit to produce them, and there's enough miners producing that the price to purchase should be close to the cost to produce. If it were any higher, competition among the miners would bid down the price. If it were any lower, the miners would exit the market and not produce anything.

It's the Week 2 bits that seem problematic to me. Unlike the Week 1 bits, there's no inherent value in them, since the notes don't specify how many of them are required to make good on the note. Unlike the Week 3 bits, no more can be produced (since it's no longer Week 2), so competition among the producers can't serve to bring the price down to their production cost. The cost to produce them is now a sunk cost. Issuers have no reason to buy them at any price, so miners should be satisfied to sell them at any price, even at a loss.

But suppose for a moment that for whatever reason, the market has run out of Week 1 and Week 3 bits, so that an issuer is forced to buy Week 2 bits to redeem a note. Now observe: the issuer is going to spend a total of $1 *no matter how many bits he buys*. The note has a face value of 100 Week 1 bits, which in turn has a value of $1. If the issuer pays a penny each, he has to buy 100. If he pays half a cent each, he buys 200. If he pays two cents each, he buys 50. *The price of Week 2 bits is decoupled from any external factor that would limit either the bid or ask price in either direction.*

This is what I was thinking of when I said that there's something left unspecified. What am I missing here?

10:48 PM

Anonymous said...

Question: what is the mean IQ of the posters on the following thread.

http://www.quora.com/Bitcoin/Is-the-cryptocurrency-Bitcoin-a-good-idea

Btw, why isn't Bitcoin integrated into P2P cloud? It would seem using bitcoin token as a way to settle accounts for equal trading of digital p2p products and services would largely negate the problem of converting bitcoins to a fiat currency.

Example: I download (consume) 1 GB and upload (produce) 2 GB. I get 1 GB worth of bitcoins. I use 500 MB worth of bitcoins to download 500 MB worth of pron instead of converting it to us dollars and then using the dollars to buy 500 MB of pron. My pron dealer likes this because it doesn't need to share 14.5% cut with CCBill or it's webhost, but rather uses the 500 MB worth of bitcoins to pay the p2p network to host, distribute, authenticate, load balance and route it's content. Add a P2P DRM protocol in their and now we're smoking.

If somebody wants to write me a bittorrent distro that uses bitcoin as a token in a metered payment utility I'll use that instead of the Leechware I'm now using. And screw the World Grid altruism BS. I've got a pron addiction to feed.

My captcha: **ameme**

http://www.blogger.com/captcha?token=AM2hDkBooSCq8rnNm5DZQSNOir35W8q9ULEgHI9rgP7YdF6TDzcY0rc98IKhMx%2B56mkNmVVbVe9Wf0PYa6%2FjpURG8v2gNfBLvIdIAB26hfOqeTymmdHHF2ACnJbjqx2qPdAbkbZn6w5S

5:30 PM

Anonymous said...

Btw, what would be the going rate in bitcoins for access to a bittorrent folder on my tor-freenet-i2p-anonproxy-supercomputer filled with 20,000 .par2 parchive files which can complete offline all those multi-GiB torrents stuck at 95-99.5%?

5:47 PM

Anonymous said...

"Yet another idea: use the Bitcoin code to implement secure property titles."

Digital collectibles, unique one-of-a-kind p2p game pieces (custom character designs, weapons etc), drm brown bag wrappers for my pron. Resell mp3 downloads (and everything else) legally just like selling audio CDs at a garage sale.

7:35 PM

Anonymous said...

Regarding deflation, attrition and hoarding. I believe there is a possible solution for these. Here is my suggestion. I really hope someone with the technical skills that I don't have will implement this one day.

Make the digital currency have a lifespan. I like to call this live money or living money.

Say you 'mined' 1 coin today. The coin will 'erode' at a pre-defined rate, say 1% a day for example, or another more appropriate rate. Tomorrow the coin will be reduced to 0.99 and 0.01 goes back into the mining pool. This goes on until, if you don't spend it, the whole coin is returned to the system.

This way the huge disparity between the early adopters and the late adopters would be reduced. And even if the first miner got a million coins, the number would go down eventually and they wouldn't be able to hoard them forever.

Also, if people lost their wallets, eventually that money would all go back into the system too.

Even with a pre-defined finite number of coins, this would greatly discourage hoarding, would end the problem of attrition altogether and possibly end the problem of deflation too.

I believe the biggest problem with all currencies is the encouragement of hoarding. If you buy a car it gets old and loses value, if you buy an apple and don't eat it it rots. Banks notes get old too but then the government prints more and creates the illusion that money lasts forever.

What we need is a system of money transfer not of money making. Because of the design of bitcoin, there are many people using it to try to get rich, and not as a currency.

Unfortunately, as it is, bitcoin ends up being similar to a pyramid scheme, because the early adopters benefit a lot more than the late adopters. It then becomes about who has more money and the benefits of a decentralised currency are overshadoweded.

5:38 PM

Anonymous said...

When I said coin lifespan, I should have said decomposing rate. Meaning, whatever the amount of money you have, it goes down at a constant pre-defined rate, regardless of when it was minted. So there wouldn't be a question of having old or fresh batches of money.

Probably the decomposing rate would have to be very low to be considered acceptable, but the idea wouldn't be too different than trading livestock and vegetables. It would be sort of a slowly perishable money.

Money shouldn't last forever, because this is what encourages hoarding. I believe that it is the encouragement of hoarding that is what creates inflation and deflation problems, and inequality.

5:42 AM

Anonymous said...

Apparently, the idea of a currency that expires with time is not a new idea. They call this demurrage. Silvio Gesell, who is now dead, had the idea of an unhoardable money that he called Freigeld (which means free money in German). Reportedly, this was used in the town of Wörgl in Austria during the Great Depression with a lot of success until the national bank forced them to stop it.

2:59 PM

nazgulnarsil said...

So I had a thought about cryptographically secure titles of ownership.

Let's say we make a public-private key pair that is a hash of some uniquely identifying biometric data. Much like namecoin we then use the blockchain to encode information, specifically contracts. You can sign contracts with your private key and anyone can check what contracts you've signed with your public key. This allows you to reliably signal certain sorts of intentions and know that everyone knows that you are signalling these intentions.

9:58 PM

cunicula said...

Look at this:
https://en.bitcoin.it/wiki/Proof_of_Stake

It address your concern about the agency problem. Separating ownership from control of mining is a big problem. There is relatively simple outline here explaining why it's a problem and how it could be fixed. Unfortunately, there isn't any developer interest in this at the moment. A nice blog post from someone like you might help.

8:45 PM

Nurulbitcoin88 said...

I would like to thank you for the efforts
you have put in writing this blog. I'm hoping the same high-grade web site
post from you in the future also. Actually your creative writing abilities
has encouraged me to get my own web site going now.Really blogging is
spreading its wings and growing fast. Your write up is a great example.

4:22 AM

gwern said...

Emailing because presumably you don't obsessively watch every comment (otherwise there wouldn't be so many spam comments...)

http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html

> not just about the security technologies gwern lists (and I'm afraid the list misses one of the biggest ones, Byzantine-resilient peer-to-peer replication)

Good point. I'll add that one. But as far as I know, both peer to peer and Byzantine algorithms are no later than the '90s, even excluding Usenet or FidoNet.

> Bitcoin is not a list of cryptographic features, it's a very complex system of interacting mathematics and protocols in pursuit of what was a very unpopular goal.

'Very unpopular' is kind of my main explanation, is it not?

> (1) only a few people had read of the bit gold ideas, which although I came up with them in 1998 (at the same time and on the same private mailing list where Dai was coming up with b-money -- it's a long story) were mostly not described in public until 2005, although various pieces of it I described earlier, for example the crucial Byzantine-replicated chain-of-signed-transactions part of it which I generalized into what I call secure property titles.

Thanks for the historical detail; I was sure that 2001 or 2005 couldn't be the right date...

So. According to your post, the main blocking factors were:

1. ideological beliefs about the nature of money (liberals not interested in non-state currencies, and Austrians believing that currencies must have intrinsic value)
2. obscurity of bit gold-like ideas
3. "requiring a proof-of-work to be a node in the Byzantine-resilient peer-to-peer system to lessen the threat of an untrustworthy party controlling the majority of nodes and thus corrupting a number of important security features"
4. some simplification (not markets for converting "old" & harder-to-mine bitcoins to "new" & easier-to-mine bitcoins, but a changing network-wide consensus on how hard bitcoins must be to mine)

My own belief is that #1 is probably a significant factor, #2 may be irrelevant as all digital cryptographic currency ideas are obscure (for example, Satoshi's whitepaper does not cite bit gold but b-money, and Wei Dai does not believe his b-money influenced Bitcoin[^Dai]), and #3-4 are details which cannot possibly explain why Bitcoin has succeeded to any degree while ideas like bit gold

languished.

[^Dai]: Wei Dai, [25 February 2011](http://lesswrong.com/lw/4cs/making_money_with_bitcoin/3lq1):

> ...If you read the Wikipedia article, you should know that I didn't create Bitcoin but only described a similar idea more than a decade ago. And my understanding is that the creator of Bitcoin, who goes by the name Satoshi Nakamoto, didn't even read my article before reinventing the idea himself. He learned about it afterward and credited me in his paper. So my connection with the project is quite limited.

10:43 AM

Sonali said...

Thanks for your posts, I would be waiting for similar interesting posts in future.

Thanks
Marcus White Lisdoonvarna

9:19 AM

Doug said...

Nick,

Thanks for your great work! it is illuminating and ground breaking. I have a question regarding difficulty. Do you think it's possible to adjust difficulty automatically to follow Moore's law on a schedule? Then have the release rate of coin be inversely proportional to the total hash rate of the mining. This way you have Moore's law protection of the consensus, the ability to have greater release of coin early in the cycle and control of coin release relative to popularity. This may make excessive work less incentivized and strategic work more incentivized.

Thanks,
Doug

10:27 PM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.